



Utilisation de la fédération des identités

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

- Utilisation de la fédération des identités. 1
 - Configuration d'un référentiel d'identité fédéré 1
 - Forcer la synchronisation avec le référentiel d'identité 5
 - Désactivation de la fédération des identités. 5

Utilisation de la fédération des identités

L'utilisation de la fédération des identités accélère la configuration des groupes de locataires et des utilisateurs, et permet aux utilisateurs de se connecter au compte du locataire à l'aide des identifiants familiers.

- ["Configuration d'un référentiel d'identité fédéré"](#)
- ["Forcer la synchronisation avec le référentiel d'identité"](#)
- ["Désactivation de la fédération des identités"](#)

Configuration d'un référentiel d'identité fédéré


Vous pouvez configurer la fédération des identités si vous souhaitez que les groupes de locataires et les utilisateurs soient gérés dans un autre système, tel qu'Active Directory, OpenLDAP ou Oracle Directory Server.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez utiliser Active Directory, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité. Si vous souhaitez utiliser un service LDAP v3 non répertorié, contactez le support technique.
- Si vous prévoyez d'utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identité doit utiliser TLS 1.2 ou 1.3.

Description de la tâche

La configuration d'un service de fédération des identités pour votre locataire dépend de la configuration de votre compte locataire. Votre locataire peut partager le service de fédération des identités configuré pour Grid Manager. Si ce message s'affiche lorsque vous accédez à la page Fédération des identités, vous ne pouvez pas configurer un référentiel d'identité fédéré distinct pour ce locataire.

 This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > identity federation**.
2. Sélectionnez **Activer la fédération d'identités**.
3. Dans la section Type de service LDAP, sélectionnez **Active Directory**, **OpenLDAP** ou **Other**.

Si vous sélectionnez **OpenLDAP**, configurez le serveur OpenLDAP. Reportez-vous aux instructions de configuration d'un serveur OpenLDAP.

Sélectionnez **autre** pour configurer les valeurs d'un serveur LDAP qui utilise Oracle Directory Server.

4. Si vous avez sélectionné **autre**, renseignez les champs de la section attributs LDAP.
 - **Nom unique utilisateur** : nom de l'attribut qui contient l'identifiant unique d'un utilisateur LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `uid` Pour OpenLDAP. Si vous

configurez Oracle Directory Server, entrez `uid`.

- **UUID d'utilisateur** : nom de l'attribut qui contient l'identifiant unique permanent d'un utilisateur LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
- **Nom unique de groupe** : nom de l'attribut qui contient l'identifiant unique d'un groupe LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `cn` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `cn`.
- **UUID de groupe** : nom de l'attribut qui contient l'identificateur unique permanent d'un groupe LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.

5. Dans la section configurer le serveur LDAP, entrez les informations de serveur LDAP et de connexion réseau requises.

- **Nom d'hôte** : le nom d'hôte du serveur ou l'adresse IP du serveur LDAP.
- **Port** : port utilisé pour se connecter au serveur LDAP. Le port par défaut de STARTTLS est 389 et le port par défaut de LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port tant que votre pare-feu est configuré correctement.
- **Nom d'utilisateur** : chemin complet du nom distinctif (DN) de l'utilisateur qui se connectera au serveur LDAP. Pour Active Directory, vous pouvez également spécifier le nom de connexion bas niveau ou le nom principal d'utilisateur.

L'utilisateur spécifié doit être autorisé à répertorier les groupes et les utilisateurs et à accéder aux attributs suivants :

- `sAMAccountName` ou `uid`
- `objectGUID`, `entryUUID`, ou `nsuniqueid`
- `cn`
- `memberOf` ou `isMemberOf`
- **Mot de passe** : mot de passe associé au nom d'utilisateur.
- **DN de base de groupe** : chemin complet du nom distinctif (DN) pour une sous-arborescence LDAP que vous voulez rechercher des groupes. Dans l'exemple Active Directory (ci-dessous), tous les groupes dont le nom unique est relatif au DN de base (`DC=storagegrid,DC=exemple,DC=com`) peuvent être utilisés comme groupes fédérés.

Les valeurs **Nom unique de groupe** doivent être uniques dans le **DN de base de groupe** auquel elles appartiennent.

- **DN de base d'utilisateur** : le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP que vous voulez rechercher des utilisateurs.

Les valeurs **Nom unique utilisateur** doivent être uniques dans le **DN de base utilisateur** auquel elles appartiennent.

6. Dans la section **transport Layer Security (TLS)**, sélectionnez un paramètre de sécurité.

- **Utilisez STARTTLS (recommandé)** : utilisez STARTTLS pour sécuriser les communications avec le

serveur LDAP. Il s'agit de l'option recommandée.

- **Utilisez LDAPS** : l'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Cette option est prise en charge pour des raisons de compatibilité.
- **N'utilisez pas TLS** : le trafic réseau entre le système StorageGRID et le serveur LDAP ne sera pas sécurisé.

Cette option n'est pas prise en charge si votre serveur Active Directory applique la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

7. Si vous avez sélectionné STARTTLS ou LDAPS, choisissez le certificat utilisé pour sécuriser la connexion.

- **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser les connexions.
- **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat de sécurité personnalisé.

Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

8. Sélectionnez **Tester la connexion** pour valider vos paramètres de connexion pour le serveur LDAP.

Un message de confirmation s'affiche dans le coin supérieur droit de la page si la connexion est valide.

9. Si la connexion est valide, sélectionnez **Enregistrer**.

La capture d'écran suivante montre des exemples de valeurs de configuration pour un serveur LDAP qui utilise Active Directory.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

OpenLDAP

Other

Configure LDAP server (All fields are required)

Hostname

my-active-directory.example.com

Port

389

Username

MyDomain\Administrator

Password

••••••••

Group Base DN

DC=storagegrid,DC=example,DC=com

User Base DN

DC=storagegrid,DC=example,DC=com

Informations associées

["Autorisations de gestion des locataires"](#)

["Instructions de configuration d'un serveur OpenLDAP"](#)

Instructions de configuration d'un serveur OpenLDAP

Si vous souhaitez utiliser un serveur OpenLDAP pour la fédération des identités, vous devez configurer des paramètres spécifiques sur le serveur OpenLDAP.

Recouvrements de memberOf et de raffint

Les recouvrements de membre et de raffinage doivent être activés. Pour plus d'informations, reportez-vous

aux instructions relatives à la maintenance de l'adhésion inverse au groupe dans le Guide de l'administrateur pour OpenLDAP.

Indexation

Vous devez configurer les attributs OpenLDAP suivants avec les mots-clés d'index spécifiés :

```
olcDbIndex: objectClass eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: cn eq,pres,sub
olcDbIndex: entryUUID eq
```

De plus, assurez-vous que les champs mentionnés dans l'aide pour le nom d'utilisateur sont indexés pour des performances optimales.

Reportez-vous aux informations sur la maintenance de l'adhésion au groupe inverse dans le Guide de l'administrateur pour OpenLDAP.

Forcer la synchronisation avec le référentiel d'identité

Le système StorageGRID synchronise régulièrement les groupes fédérés et les utilisateurs à partir du référentiel d'identité. Vous pouvez forcer la synchronisation à démarrer si vous souhaitez activer ou restreindre les autorisations utilisateur le plus rapidement possible.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Le référentiel d'identité enregistré doit être activé.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > identity federation**.

La page fédération des identités s'affiche. Le bouton **Sync Server** se trouve en haut à droite de la page.



Si le référentiel d'identité enregistré n'est pas activé, le bouton **Sync Server** n'est pas actif.

2. Sélectionnez **serveur de synchronisation**.

Un message de confirmation s'affiche pour indiquer que la synchronisation a démarré correctement.

Informations associées

["Autorisations de gestion des locataires"](#)

Désactivation de la fédération des identités

Si vous avez configuré un service de fédération des identités pour ce locataire, vous

pouvez désactiver temporairement ou définitivement la fédération des identités pour les groupes de locataires et les utilisateurs. Lorsque la fédération des identités est désactivée, il n'y a aucune communication entre le système StorageGRID et le référentiel d'identité. Cependant, tous les paramètres que vous avez configurés sont conservés, ce qui vous permet de réactiver facilement la fédération d'identités à l'avenir.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Avant de désactiver la fédération des identités, vous devez prendre connaissance des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conserveront l'accès au compte du locataire jusqu'à l'expiration de leur session, mais ils ne pourront pas se connecter après l'expiration de leur session.
- La synchronisation entre le système StorageGRID et le référentiel d'identité ne se fera pas.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > identity federation**.
2. Décochez la case **Activer la fédération d'identités**.
3. Sélectionnez **Enregistrer**.

Informations associées

["Autorisations de gestion des locataires"](#)

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.